United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Wednesday,
July 26, 2000

CRITICAL INFRASTRUCTURE PROTECTION

Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

G A O
Accountability * Integrity * Reliability

GAO/T-AIMD-00-268

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the challenges of providing a coordinated response to computer security threats. As you know, computer security risks have increased dramatically over the last decade as our government and our nation have become ever more reliant on interconnected computer systems to support critical operations and infrastructures, including telecommunications, finance, power distribution, emergency services, law enforcement, national defense, and other government services. These interconnected systems are part of a global information infrastructure that is not defined by geographic boundaries or by unity of purpose among the individual components of the infrastructure. To a large extent, these components are developed and maintained by private companies and, in some cases, foreign entities. This situation is challenging nations to consider new strategies for protecting sensitive data and information-based assets, in part through information sharing and coordination between public and private organizations–sometimes on an international scale.

Today, I would like to discuss the challenges to achieving effective coordination that we have identified over the last 2 years. Such challenges–which include establishing trust relationships between the government and private sector, developing the mechanisms of gathering and sharing data, strengthening technical capabilities, and providing stronger governmentwide leadership and continuity for critical infrastructure protection–need to be successfully addressed in order to institute effective information sharing and coordination mechanisms among individual components of the infrastructure.

Increasing Need for Coordinated Response

Since the early 1990s, the unprecedented growth in computer interconnectivity, most notably growth in use of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous in terms of facilitating communications, business processes, and access to information. However, without proper safeguards, this widespread interconnectivity poses enormous risks to our computer systems and, more importantly, to the critical operations and infrastructures they support.

While attacks to date have not caused widespread or devastating disruptions, the potential for more catastrophic damage is significant. Official estimates show that over 100 countries already have or are developing computer attack capabilities. Hostile nations or terrorists

could use cyber-based tools and techniques to disrupt military operations, communications networks, and other information systems or networks. The National Security Agency has determined that potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems. According to Defense officials, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. According to a leading security software designer, viruses in particular are becoming more disruptive for computer users. In 1993 only about 10 percent of known viruses were considered destructive, harming files and hard drives. But now about 35 percent are regarded as harmful.

Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to these threats.

- First, having information on threats and on actual incidents experienced by others can help an organization better understand the risks it faces and determine what preventative measures should be implemented.
- Second, more urgent, real-time warnings can help an organization take immediate steps to mitigate an imminent attack.
- Lastly, information sharing and coordination are important after an attack has occurred to facilitate criminal investigations, which may cross jurisdictional boundaries. Such after-the-fact coordination could also be useful in recovering from a devastating attack, should such an attack ever occur.

The recent episode of the ILOVEYOU computer virus in May 2000, which affected governments, corporations, media outlets, and other institutions worldwide, highlighted the need for greater information sharing and coordination. Because information sharing mechanisms were not able to provide timely enough warnings against the impending attack, many entities were caught off guard and forced to take their networks off-line for hours. Getting the word out within some federal agencies themselves also proved difficult. At the Department of Defense, for example, the lack of teleconferencing capability slowed the response effort because Defense components had to be called individually. The National Aeronautics and Space Administration (NASA) had difficulty communicating warnings when e-mail services disappeared, and while backup communication mechanisms are in place, NASA officials told us that they are rarely tested. We also found that the few federal components that either discovered or

were alerted to the virus early did not effectively warn others. For example, officials at the Department of the Treasury told us that the U.S. Customs Service received an Air Force Computer Emergency Response Team (AFCERT) advisory early in the morning of May 4, but that Customs did not share this information with other Treasury bureaus.

Current Information Sharing and Coordination Efforts

The federal government recognized several years ago that addressing computer-based risks to our nation's critical infrastructures required coordination and cooperation across federal agencies and among public- and private-sector entities and other nations. In May 1998, following a report by the President's Commission on Critical Infrastructure Protection that described the potential devastating implications of poor information security from a national perspective, the government issued Presidential Decision Directive (PDD) 63. Among other things, this directive tasked federal agencies with developing critical infrastructure protection plans and establishing related links with private industry sectors. It also required that certain executive branch agencies assess the cyber vulnerabilities of the nation's critical infrastructures—information and communications; energy; banking and finance; transportation; water supply; emergency services; law enforcement; and public health, as well as those authorities responsible for continuity of federal, state, and local governments.

A variety of activities have been undertaken in response to PDD 63, including development and review of individual agency critical infrastructure protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links. In January 2000 the White House released its *National Plan for Information Systems Protection*[1] as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan focuses largely on federal efforts being undertaken to protect the nation's critical cyber-based infrastructure. Subsequent versions are to address protecting other elements of the nation's infrastructure, including those pertaining to the physical infrastructure and specific roles and responsibilities of state and local governments and the private sector.

Moreover, a number of government and private sector organizations have already been established to facilitate information sharing and coordination. These range from groups that disseminate information on

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue,* The White House, January 7, 2000.

immediate threats and vulnerabilities, to those that seek to facilitate public-private sector information sharing on threats pertaining to individual infrastructure sectors, and those that promote coordination on an international scale.

At the federal level, for example, the National Infrastructure Protection Center (NIPC), located at the Federal Bureau of Investigation (FBI), is to serve as a focal point in the federal government for gathering information on threats as well as facilitating and coordinating the federal government's response to incidents impacting key infrastructures. It is also charged with issuing attack warnings to private sector and government entities as well as alerts to increases in threat conditions. The Federal Computer Incident Response Capability (FedCIRC) is a collaborative partnership of computer security and law enforcement professionals established to handle computer security incidents and to provide both proactive and reactive security services for the federal government. In addition, the National Institute of Standards and Technology (NIST) is working to facilitate information sharing in the security community by building a database containing detailed information on computer attacks and the Critical Infrastructure Assurance Office (CIAO) is working to coordinate private sector participation in information gathering in the area of cyber assurance. The Administration is also undertaking efforts to facilitate information sharing with other nations.

Examples of other organizations focusing on information sharing and coordination include the following:

- Carnegie Mellon University's CERT Coordination Center,[2] which is charged with establishing a capability to quickly and effectively coordinate communication among experts in order to limit damage, respond to incidents, build awareness of security issues across the Internet community.

- The System Administration, Networking, and Security (SANS) Institute, which is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions for challenges they face.

[2]Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency.

- The National Coordinating Center for Telecommunications, which is a joint industry/government organization that is focusing on facilitating information sharing between the telecommunications industry and government.
- The Financial Services Information Sharing and Analysis Center, which is a similar organization that exclusively serves the banking, securities, and insurance industries.
- Agora, which is a forum that is composed more than 300 people from approximately 100 companies and 45 government agencies, including Microsoft, Blue Shield, the FBI, U.S. Secret Service, U.S. Customs Service agents, and the Royal Canadian Mounted Police as well as local police, county prosecutors, and computer professionals from the Pacific Northwest. Members voluntarily share information on common computer security problems, best practices to counter them, protecting electronic infrastructures, and educational opportunities.
- The Forum of Incident Response and Security Teams (FIRST), which provides a closed forum for incident response and security teams from 19 countries to share experiences, exchange information related to incidents, and promote preventative activities.
- The International Organization on Computer Evidence, which provides an international forum for law enforcement agencies to exchange information concerning computer crime investigation and related forensic issues.

Challenges to Effective Coordination

Developing the information sharing and coordination capabilities needed to effectively deal with computer threats and actual incidents is complex and challenging but essential. Data on possible threats–ranging from viruses, to hoaxes, to random threats, to news events, and computer intrusions–must be continually collected and analyzed from a wide spectrum of globally distributed sources. Moreover, once an imminent threat is identified, appropriate warnings and response actions must be effectively coordinated among government agencies, the private sector, and, when appropriate, other nations. It is important that this function be carried out as effectively, efficiently, and quickly as possible in order to ensure continuity of operations as well as minimize disruptions.

At the same time, it is not possible to build an overall, comprehensive picture of activity on the global information infrastructure. Networks themselves are too big, they are growing too quickly, and they are continually being reconfigured and reengineered. As a result, it is essential that strong partnerships be developed between a wide range of

stakeholders in order to ensure that the right data are at the right place at the right time.

Creating partnerships for information sharing and coordination is a formidable task. Trust needs to be established among a broad range of parties with varying interests and expectations, procedures for gathering and sharing information need to be developed, and technical issues need to be addressed. Moreover, if the federal government itself is going to be a credible player in response coordination, it needs to have its own systems and assets well protected. This means overcoming significant and pervasive security weaknesses at each of the major federal agencies and instituting governmentwide controls and mechanisms needed to provide effective oversight, guidance, and leadership. Perhaps most importantly, this activity needs to be guided by a comprehensive strategy to ensure that it is effective, to avoid unnecessary duplication of effort, and to maintain continuity.

I would like to discuss each of these challenges in more detail as successfully addressing them is essential to getting the most from information sharing mechanisms currently operating as well as establishing new ones.

Establishing Trust Relationships

A key element to the success of information sharing partnerships is developing trusted relationships among the broad range of stakeholders involved with critical infrastructure protection. (See figure 1 for examples of these stakeholders). Jointly-designed, built, and staffed mechanisms among involved parties is most likely to obtain critical buy-in and acceptance by industry and others. Each partner must ensure the sharing activity is equitable and that it provides a value added to the cost of information sharing. However, this can be difficult in the face of varying interests, concerns, and expectations. The private sector, for example, is motivated by business concerns and profits, whereas the government is driven by national and economic security concerns. These disparate interests can lead to profoundly different views and perceptions about threats, vulnerabilities, and risks, and they can affect the level of risk each party is willing to accept and the costs each is willing to bear.

Moreover, as we testified before this Subcommittee in June,[3] concerns have been raised that industry could potentially face antitrust violations

[3] *Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000* (GAO/T-AIMD-00-229, June 22, 2000).

for sharing information with other industry partners, subject their information the Freedom of Information Act (FOIA) disclosures or face potential liability concerns for information shared in good faith. Further, there is a concern that an inadvertent release of confidential business material, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms.

Some of these concerns are addressed by this Subcommittee's proposed Cyber Security Information Act of 2000 (H.R. 4246). Specifically, the bill would protect information being provided by the private sector from disclosure by federal entities under FOIA or disclosure to or by any third party. It would prohibit the use of information by any federal and state organization or any third party in any civil actions. And it would enable the President to establish and terminate working groups composed of federal employees for the purposes of engaging outside organizations in discussions to address and share information about cyber security. By removing these concerns about sharing information on critical infrastructure threats, H.R. 4246 can facilitate private-public partnerships and help spark the dialogue needed to identify threats and vulnerabilities and to develop response strategies.

For several reasons, the private sector may also have reservations about sharing information with law enforcement agencies. For example, law enforcement entities have strict rules regarding evidence in order to preserve its integrity for prosecuting cases. Yet, complying with law enforcement procedures can be costly because it requires training, implementing proper auditing and control mechanisms, and following proper procedures. Additionally, a business may not wish to report an incident if it believes that its image might be tarnished.

For national security reasons, the government itself may be reluctant to share classified information that could be of value to the private sector in deterring or thwarting electronic intrusions and information attacks. Moreover, declassifying and sanitizing such data takes time, which could affect time-critical operations. Nevertheless, until the government provides detailed information on specific threats and vulnerabilities, the private sector will not be able to build a business case to justify information sharing and will likely remain reluctant to share its own information.

Figure 1: Examples of Stakeholders in Information Sharing Efforts

- The public and internet community at large
- Law enforcement
- Government agencies
- The national security and intelligence communities
- Providers of network and other key infrastructure services
- Technology and security product vendors
- Security experts
- Incident response teams
- Education and research communities
- International standard-setting bodies
- Media

Establishing Reporting Needs and Communication Mechanisms

A significant amount of work still needs to be done just in terms of ensuring that the right type of information is being collected and that there are effective and secure mechanisms for collecting, analyzing, and sharing it. This requires agreeing, in advance, on the types of data to be collected and reported as well as on the level of detail. Again, this can be difficult given varying interests and expectations. The private sector, for example, may want specific threat or vulnerability information so that immediate actions can be taken to avert an intrusion. Law enforcement agencies may want specific information on perpetrators and particular aspects of the attack, as well as the intent of the attack and the consequences of or damages due to the attack. At the same time, many computer security professionals may want the technical details that enable a user to compromise a computer system in order to determine how to detect such actions.

After determining what types of information to collect and report, guidelines and procedures need to be established to effectively collect and disseminate data and contact others during an incident. Among other things, this involves identifying the best mechanisms for disseminating advisories and urgent notices, such as e-mail, fax, voice messages, pagers, or cell phones; designating points-of-contact; identifying the specific responsibilities of information-sharing partners; and deciding whether and how information should be shared with outside organizations.

Working through these and other issues has already proven to be a formidable task for some information-sharing organizations. According to the CERT Coordination Center, for example, it has taken years for incident response and security teams to develop comprehensive policies and procedures for their own internal operations because there is little or no experience on which to draw from. Moreover, the incident response team community as a whole is lacking in policies and procedures to support operations among teams. According to the Center, progress typically comes to a halt when teams become overwhelmed by the number of issues that need to be addressed before they can reach agreement on basic factors such as terminology, definitions, and priorities.

Developing Needed Technical Capabilities

Significant resources, knowledge, skills, and abilities clearly need to be brought together to develop mechanisms that can quickly and accurately collect, correlate, and analyze information and coordinate response efforts. But presently, there is a shortage of such expertise. At the federal level, for example, we have observed a number of instances where agency staff did not even have the skills needed to carry out their own computer security responsibilities or to oversee contractor activities. Additionally, according to the CERT Coordination Center, there are not enough suitably trained staff in the incident response community to implement any effective and reliable global incident response infrastructure. The President's *National Plan for Information Systems Protection* recognizes this dilemma and proposes a program to develop a cadre of highly skilled computer science and information security personnel. As this program is implemented, it will be important for the federal government to ensure that capabilities are developed for information sharing and response mechanisms in addition to individual agency computer security programs.

At the federal level, there is also a pressing need for better computer network intrusion detection monitoring systems to detect unauthorized and possible criminal activity both within and across government agencies. Under the President's *National Plan for Information Systems Protection*, the federal government is working to design and implement

highly automated security and intrusion detection capabilities for federal systems. Such systems are to provide (1) intrusion detection monitors on key nodes of agency systems, (2) access and activity rules for authorized users and a scanning program to identify anomalous or suspicious activity, (3) enterprise-wide management programs that can identify what systems are on the network, determine what they are doing, enforce access and activity rules, and potentially apply security upgrades, and (4) techniques to analyze operating system code and other software to determine if malicious code, such as logic bombs, has been installed.

As we testified in February,[4] available tools and methods for analyzing and correlating network traffic are still evolving and cannot yet be relied on to serve as an effective "burglar alarm," as envisioned by the plan. While holding promise for the future, such tools and methods raise many questions regarding technical feasibility, cost-effectiveness, and the appropriate extent of centralized federal oversight. Accordingly, these efforts will merit close congressional oversight as they are implemented.

Making the Federal Government a Model

If our government is going to play a key role in overcoming these challenges and spurring effective information sharing and coordination, it must be a model for information security and critical infrastructure protection, which means having its own systems and assets adequately protected. Unfortunately, we have a long way to go before we can point to our government as a model for others to emulate. As noted in previous testimonies and reports, virtually every major federal agency has poor computer security. Federal agencies are at risk of having their key systems and information assets compromised or damaged from both computer hackers as well as unauthorized activity by insiders. Recent audits conducted by GAO and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, and nonexistent or weak continuity of service plans.

While a number of factors have contributed to weak federal information security, such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures, the fundamental underlying problem is poor security program management. Agencies have not established the basic management framework needed

[4] *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (GAO/AIMD-00-72, February 1, 2000).

to effectively protect their systems. Based on our 1998 study[5] of organizations with superior security programs, such a framework involves managing information security risks through a cycle of risk management activities that include (1) assessing risk and determining protection needs, (2) selecting and implementing cost-effective policies and controls to meet these needs, (3) promoting awareness of policies and controls and of the risks that prompted their adoption, and (4) implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls. Additionally, a strong central focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

While individual agencies bear primary responsibility for the information security associated with their own operations and assets, there are several areas where governmentwide criteria and requirements also need to be strengthened. Specifically, there is a need for routine, periodic independent audits of agency security programs to provide a basis for measuring agency performance and information for strengthened oversight. There is also a need for more prescriptive guidance regarding the level of protection that is appropriate for agency systems. Additionally, as mentioned earlier, gaps in technical expertise should be addressed.

Developing a Comprehensive Strategy to Ensure Effectiveness and Continuity

A comprehensive, cohesive strategy is needed to ensure that our information security and critical infrastructure protection efforts are effective and that we build on efforts already underway. However, developing and implementing such a strategy will require strong federal leadership. Such leadership will be needed to press individual federal agencies to institute the basic management framework needed to make the federal government a model for critical infrastructure protection and to foster the governmentwide mechanisms needed to facilitate oversight and guidance. In addition, leadership will be needed to ensure that the other challenges discussed today are met.

The *National Plan for Information Systems Protection* is a move towards developing such a framework. However, it does not address a broad range of concerns that go beyond federal efforts to protect the nation's critical cyber-based infrastructures. In particular, the plan does not address the international aspects of critical infrastructure protection or the specific roles industry and state and local governments will play.

[5] *Executive Guide: Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

The Administration is working toward issuing a new version of the plan this fall that addresses these issues. However, there is no guarantee that this version will be completed by then or that it will be implemented in a timely manner. Additionally, a sound long-term strategy to protect U.S. critical infrastructures depends not only on implementation of our national plan, but on appropriately coordinating our plans with those of other nations, establishing and maintaining a dialogue on issues of mutual importance, and cooperating with other nations and infrastructure owners.

An important element of such a plan will be defining and clarifying the roles and responsibilities of organizations—especially federal entities–serving as central repositories of information or as coordination focal points. As discussed earlier, there are numerous organizations currently collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents, including NIST, the NIPC, FedCIRC, the Critical Information Assurance Office, the federal CIO Council, and various units within the Department of Defense. The varying types of information and analysis that these organizations provide can be useful. However, especially in emergency situations, it is important that federal agencies and others clearly understand the roles of these organizations, which ones they should contact if they want to report a computer-based attack, and which ones they can rely on for information and assistance.

Clarifying organizational responsibilities can also ensure a common understanding of how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals. Moreover, the need for such clear delineation of responsibilities will be even more important as international cooperative relationships in this area mature. If such roles and responsibilities are not clearly defined and coordinated under a comprehensive plan, there is a risk that these efforts will be unfocused, inefficient, and ineffective.

In conclusion, a number of positive actions have already been taken to provide a coordinated response to computer security threats. In particular, the federal government is in the process of establishing mechanisms for gathering information on threats, facilitating and coordinating response efforts, sharing information with the private sector, and working to build collaborative partnerships. Other stakeholders are also working to facilitate public-private information sharing on threats in individual sectors and to promote international coordination.

Nevertheless, there are formidable challenges that need to be overcome to strengthen ongoing efforts and to work toward building a more comprehensive and effective information-sharing and coordination infrastructure. In particular, trust needs to be established among a broad range of stakeholders, questions on the mechanics of information sharing and coordination need to be resolved, roles and responsibilities need to be clarified, and technical expertise needs to be developed. Addressing these challenges will require concerted efforts by senior executives—both public and private—as well as technical specialists, law enforcement and national security officials, and providers of network services and other key infrastructure services, among others. Moreover, it will require stronger leadership by the federal government to develop a comprehensive strategy for critical infrastructure protection, work through concerns and barriers to sharing information, and institute the basic management framework needed to make the federal government a model of critical infrastructure protection.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other Members of the Subcommittee may have.

We performed our review from July 10 through July 24, 2000, in accordance with generally accepted government auditing standards. For information about this testimony, please contact Jack L. Brock, Jr., at (202) 512-6240. Jean Boltz, Cristina Chaplain, Mike Gilmore, Danielle Hollomon, Paul Nicholas, and Alicia Sommers made key contributions to this testimony.

(512012)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)